CLAIMS

What is claimed is:

1. A method for providing a secure transaction, comprising the steps of:

(a) receiving a new identification verification data by a transaction device directly from a user;

(b) storing the new identification verification data on the transaction device only, wherein the new identification verification data is not shared with another device;

(c) receiving an input of an identification verification data by the transaction device directly from the user;

(d) activating the transaction device if the inputted identification verification data matches the new identification verification data; and

(e) deactivating the transaction device when an event occurs.

2. The method of claim 1, wherein the receiving step (a) comprises:

(a1) assigning an initial identification verification data to the user;

(a2) receiving the initial identification verification data by the transaction device directly from the user;

(a3) verifying the initial identification verification data by the transaction device;

(a4) receiving an indication of a new identification verification data by the transaction device; and

(a5) receiving the new identification verification data by the transaction device directly from the user.

3. The method of claim 1, wherein the activating step (d) comprises:

(d1) determining if the inputted identification verification data matches the new identification verification data by the transaction device;

(d2) activating the transaction device if the inputted identification verification data matches the new identification verification data; and

(d3) starting a timer if the transaction device is activated, wherein the timer expires after the predetermined period of time.

4. The method of claim 3, wherein the deactivating step (e) comprises:

(e1) deactivating the transaction device when the timer expires.

5. The method of claim 1, wherein the deactivating step (e) comprises:

(e1) deactivating the transaction device when the secure transaction is completed.

6. The method of claim 1, wherein the new identification verification data comprises at least one of the following:

a personal identification number;

a fingerprint; or

a signature.

7. A method for providing a secure transaction, comprising the steps of:

(a) receiving an initial identification verification data by the transaction device directly from the user;

(b) verifying the initial identification verification data by the transaction device;

(c) receiving a new identification verification data by the transaction device directly from the user;

(d) storing the new identification verification data on the transaction device only, wherein the new identification verification data is not shared with another device;

(e) receiving an input of an identification verification data by the transaction device directly from the user;

(f) determining if the inputted identification verification data matches the new identification verification data by the transaction device;

(g) activating the transaction device if the inputted identification verification data matches the new identification verification data;

(h) starting a timer if the transaction device is activated, wherein the timer expires after a predetermined period of time; and

(i) deactivating the transaction device when the timer expires.

8. A method for providing a secure transaction, comprising the steps of:

(a) receiving an initial identification verification data by the transaction device directly from the user;

(b) verifying the initial identification verification data by the transaction device;

(c) receiving a new identification verification data by the transaction device directly from the user;

(d) storing the new identification verification data on the transaction device only, wherein the new identification verification data is not shared with another device;

(e) receiving an input of an identification verification data by the transaction device directly from the user;

(f) determining if the inputted identification verification data matches the new identification verification data by the transaction device;

(g) activating the transaction device if the inputted identification verification data matches the new identification verification data; and

(h) deactivating the transaction device when the secure transaction is completed.

9. A transaction device, comprising:

an inputting means for receiving an inputted identification verification data;

a decoder coupled to the inputting means for sensing, decoding, and verifying the inputted identification verification data; and

a processor coupled to the decoder, wherein the decoder asserts an activation signal to the processor if the identification verification data is verified, wherein the decoder de-asserts the activation signal when an event occurs.

10. The device of claim 9, wherein the event comprises a completion of a secure transaction.

11. The device of claim 9, further comprising:

a timer circuit coupled to the decoder, wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the event comprises the expiration of the timer circuit, wherein the decoder de-asserts the activation signal to the processor when the timer circuit expires.

12. The device of claim 9, wherein the inputting means comprises a plurality of capacitive keys, wherein each capacitive key comprises a first side and a second side.

13. The device of claim 9, further comprising:

an oscillator coupled to the inputting means; and

a power source coupled to the oscillator and the decoder.

14. The device of claim 9, wherein the decoder comprises a stored identification verification data, wherein the decoder verifies the inputted identification verification data by determining that the inputted identification verification data matches the stored identification verification data.

15. A transaction device, comprising:

a plurality of capacitive keys for inputting an identification verification data, wherein each capacitive key comprises a first side and a second side;

an oscillator coupled to the first side of each capacitive key;

a decoder coupled to the second side of each capacitive key for sensing, decoding, and verifying the inputted identification verification data when the first and second sides of at least one of the capacitive keys are coupled, wherein the decoder comprises a stored identification verification data, wherein the decoder verifies the inputted identification verification data by determining that the inputted identification verification data matches the stored identification verification data;

a power source coupled to the oscillator and the decoder;

a processor coupled to the decoder, wherein the decoder asserts an activation signal to the processor if the inputted identification verification data is verified; and

a timer circuit coupled to the decoder, wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the decoder de-asserts the activation signal to the processor when the timer circuit expires.

16. A transaction device, comprising:

a plurality of capacitive keys for inputting an identification verification data, wherein each capacitive key comprises a first side and a second side;

an oscillator coupled to the first side of each capacitive key;

a decoder coupled to the second side of each capacitive key for sensing, decoding, and verifying the inputted identification verification data when the first and second sides of at least one of the capacitive keys are coupled, wherein the decoder comprises a stored identification verification data, wherein the decoder verifies the inputted identification verification data by determining that the inputted identification verification data matches the stored identification verification data;

a power source coupled to the oscillator and the decoder; and

a processor coupled to the decoder, wherein the decoder asserts an activation signal to the processor if the inputted identification verification data is verified, wherein the decoder de-asserts the activation signal to the process when a secure transaction is completed.